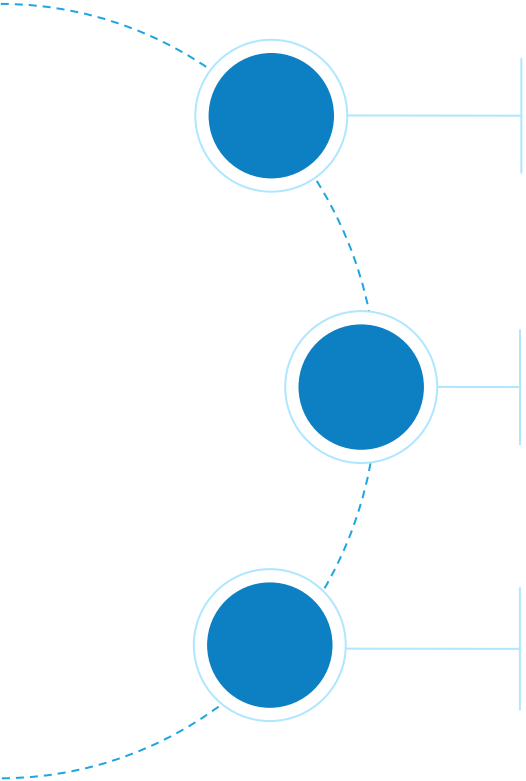
ИТРИУМ

КИБЕРЗАЩИЩЕННАЯ ПЛАТФОРМА НЕЙРОСС:

Как создать систему физической безопасности, которая не станет дырой в безопасности информационной?

ЧЕМ КОНКУРИРУЮТ РАЗРАБОТЧИКИ СБ?

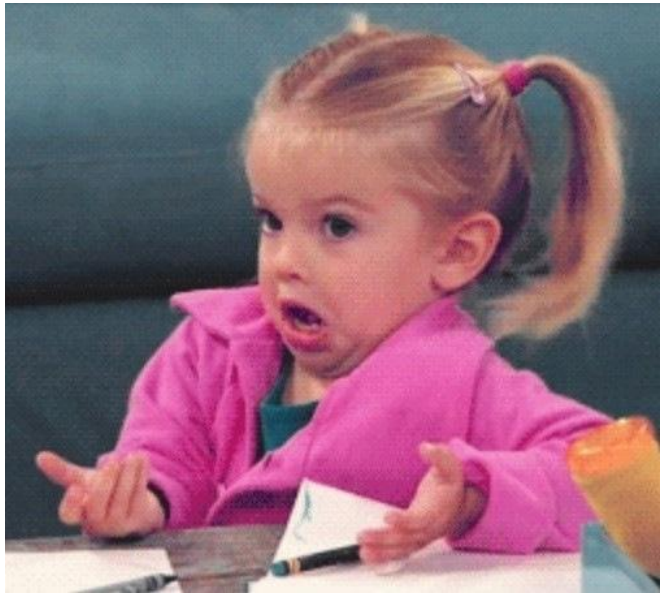


Количественные параметры

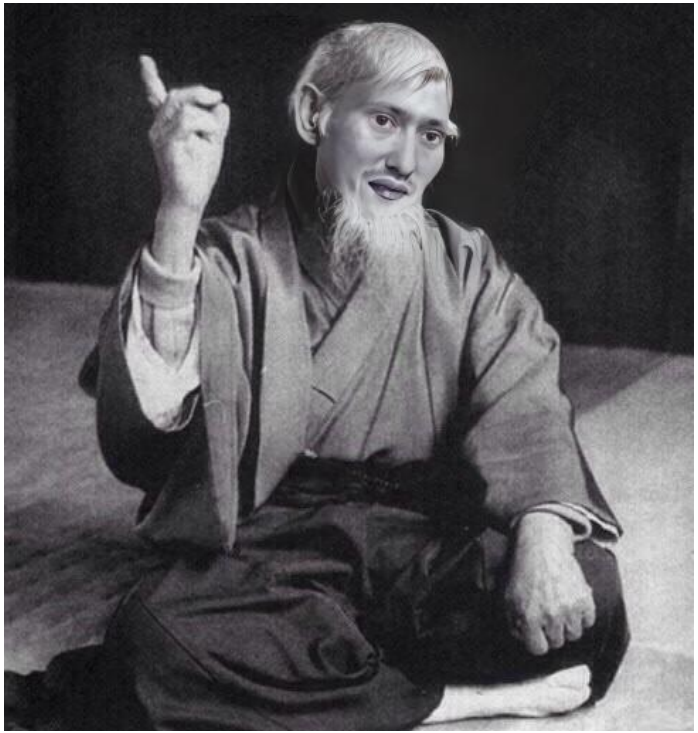
Функции по назначению

«Интуитивно-понятный интерфейс» ☺

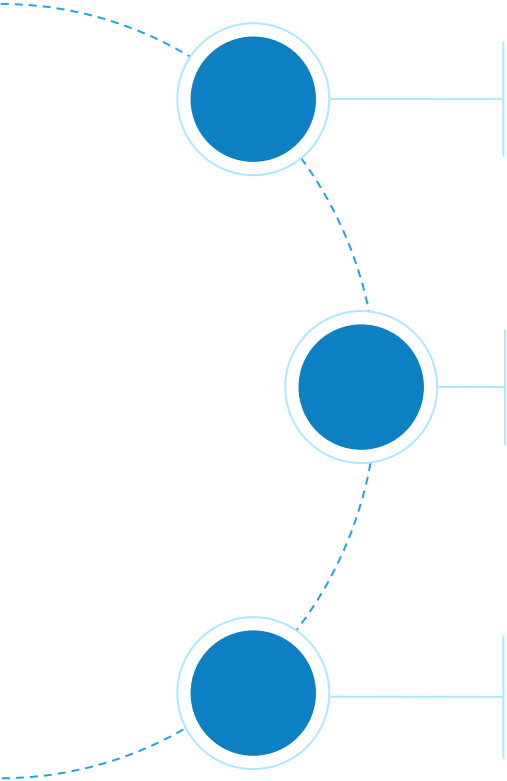
А КИБЕРЗАЩИЩЕННОСТЬ?



А КИБЕРЗАЩИЩЕННОСТЬ ОБЕСПЕЧИВАЕТСЯ ФИЗИЧЕСКОЙ ИЗОЛЯЦИЕЙ!



ЭКОНОМИЧЕСКИЙ ЭФФЕКТ СБ



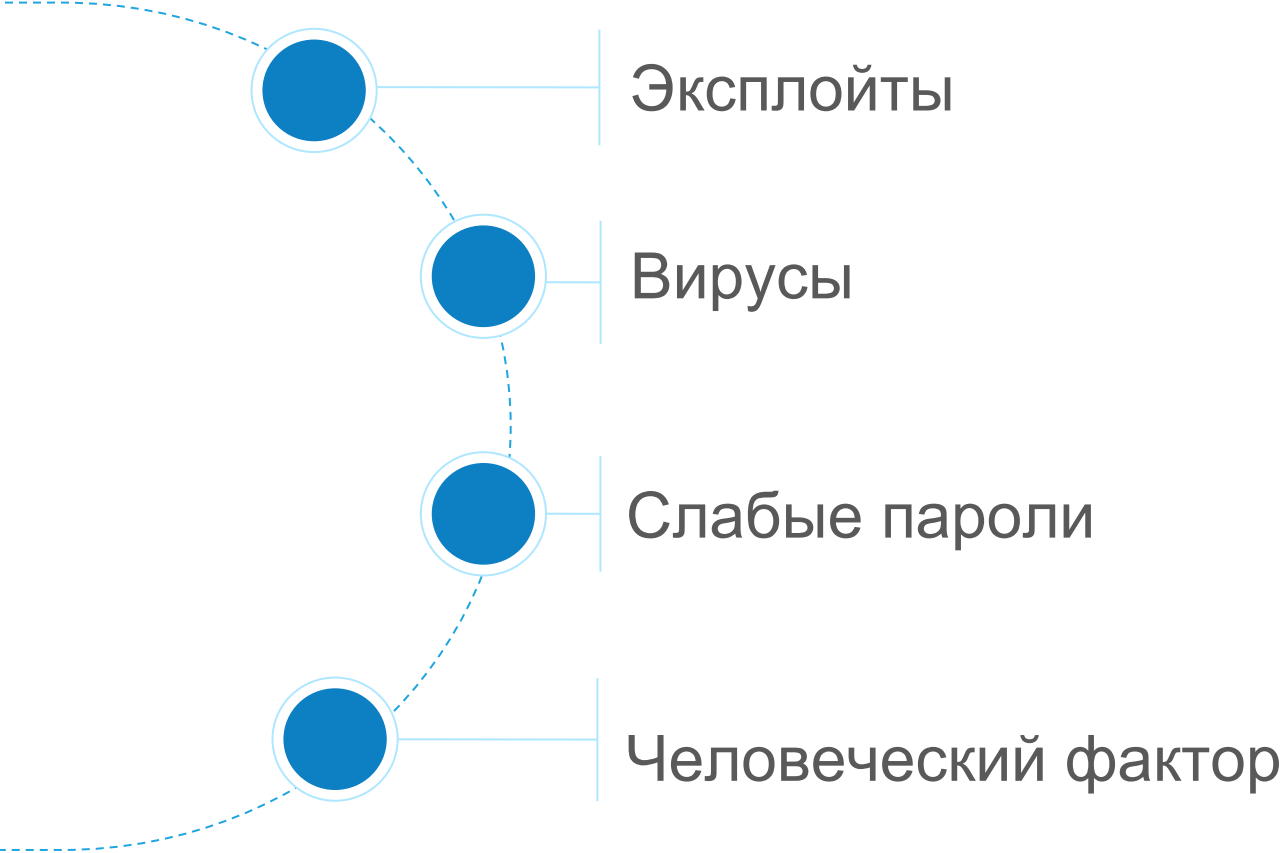
Системы все дороже

Сам по себе эффект не очевиден

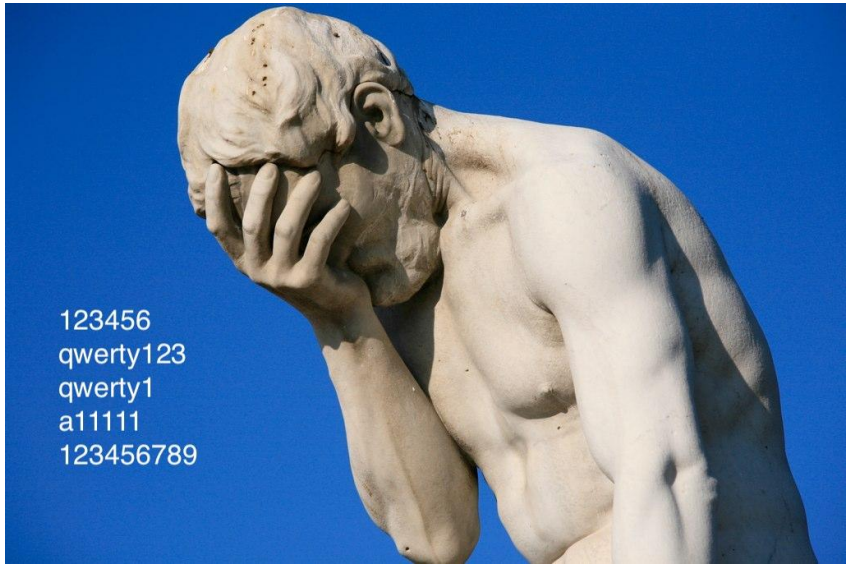
Эффект через интеграцию

А КАК ЖЕ КИБЕРЗАЩИЩЕННОСТЬ ПОСРЕДСТВОМ ИЗОЛЯЦИИ?

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УГРОЗЫ



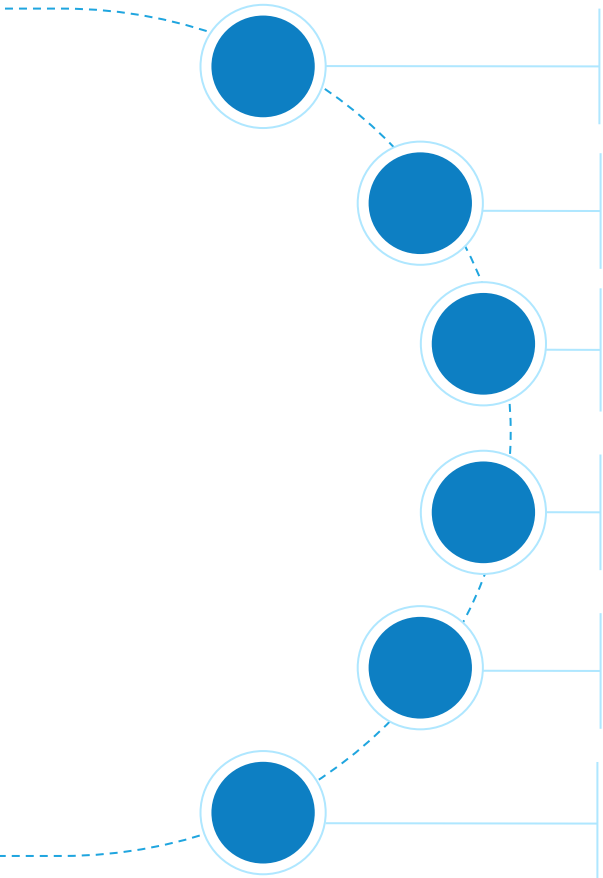
СЛАБЫЕ ПАРОЛИ – НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМАЯ «ТЕХНИЧЕСКАЯ» УЯЗВИМОСТЬ



ТИПОВОЙ ПОДХОД В СИСТЕМАХ БЕЗОПАСНОСТИ – ОГРАНИЧЕНИЕ МИНИМАЛЬНОЙ ДЛИНЫ

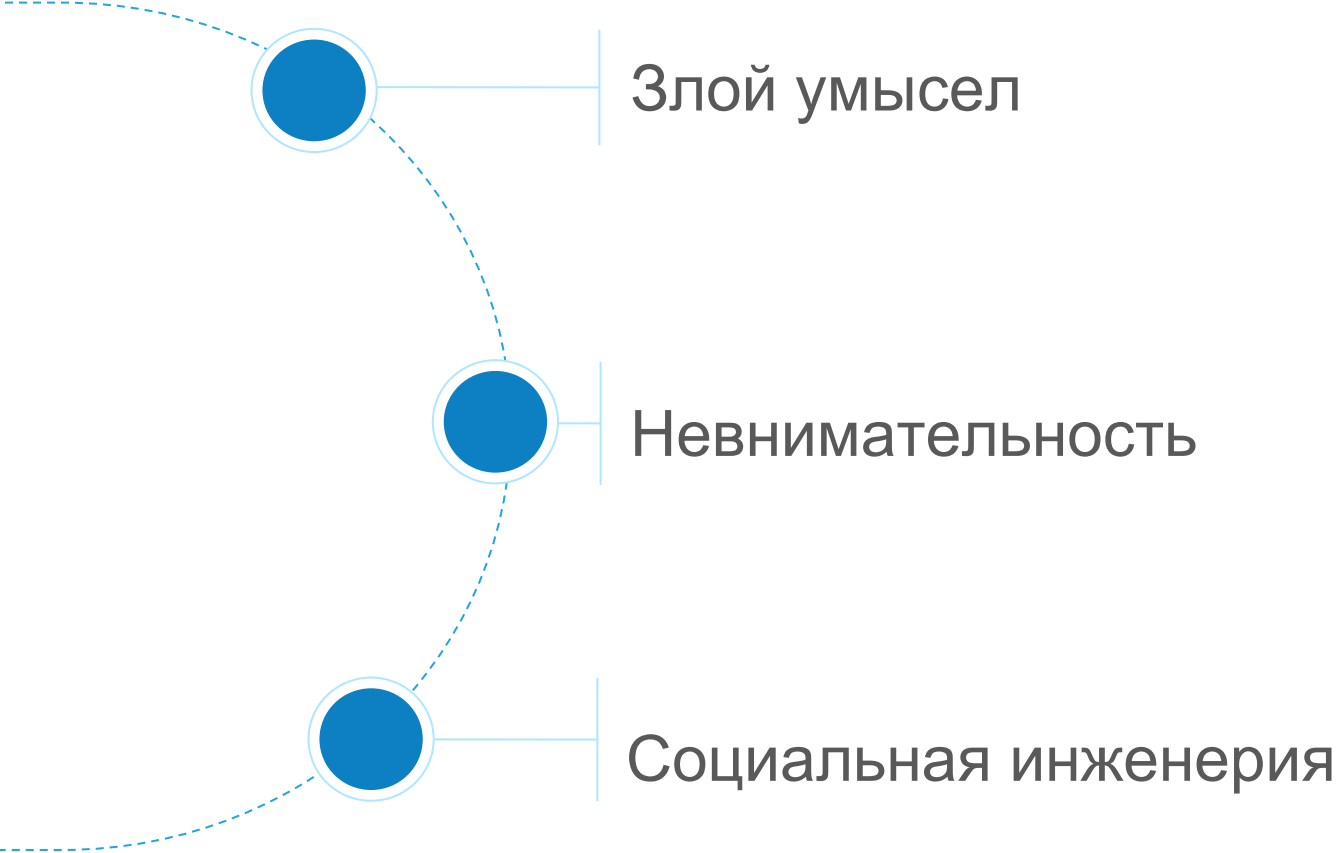
А КАК НАДО?

СИСТЕМА МЕНЕДЖМЕНТА ПАРОЛЕЙ В НЕЙРОСС

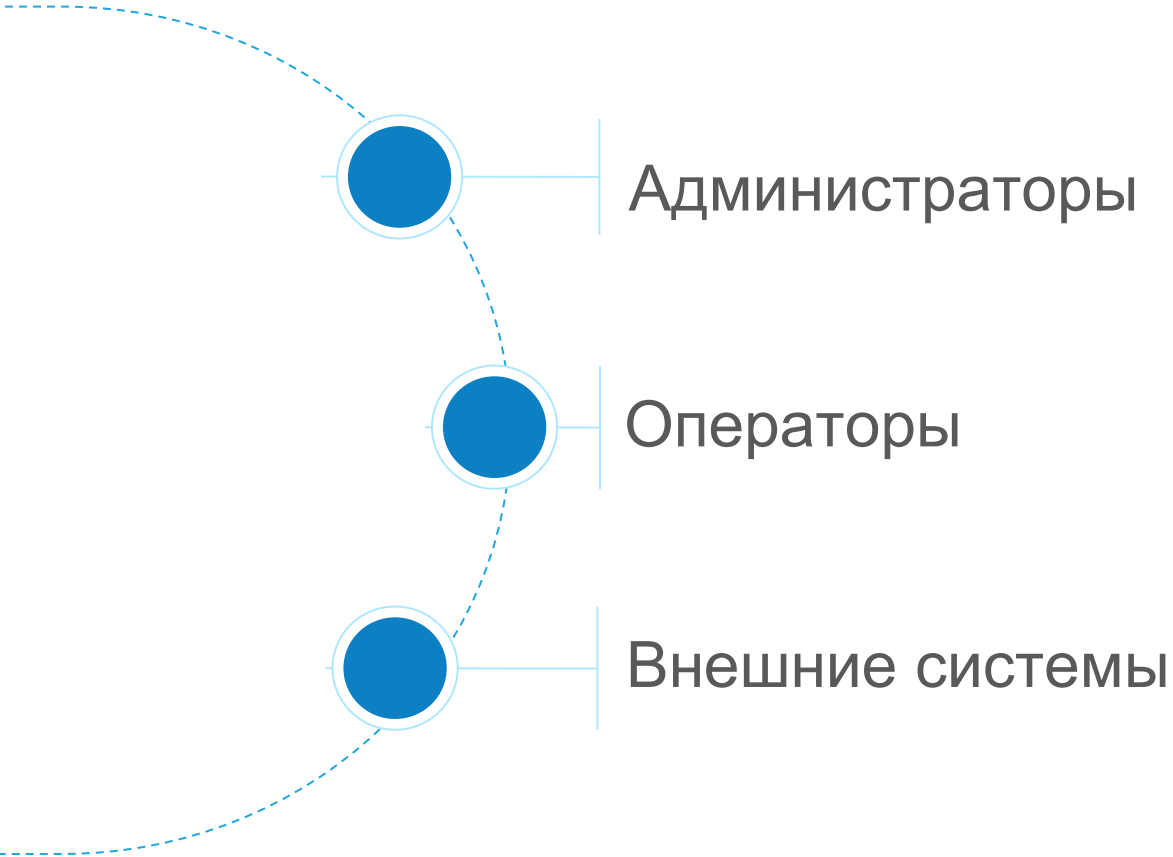


- Отказ от паролей по-умолчанию
- Контроль сложности (не только длина)
- Ротация паролей
- Двухфакторная авторизация
- Правило «Четырех глаз»
- Интеграция с корпоративными сервисами

«ЧЕЛОВЕЧЕСКИЙ ФАКТОР»



КТО РАБОТАЕТ С СИСТЕМОЙ



АДМИНИСТРАТОР В ТИПИЧНОЙ СБ: «ЦАРЬ, БОГ И ВОИНСКИЙ НАЧАЛЬНИК»

РАЗДЕЛЕНИЕ АДМИНИСТРАТИВНЫХ РОЛЕЙ

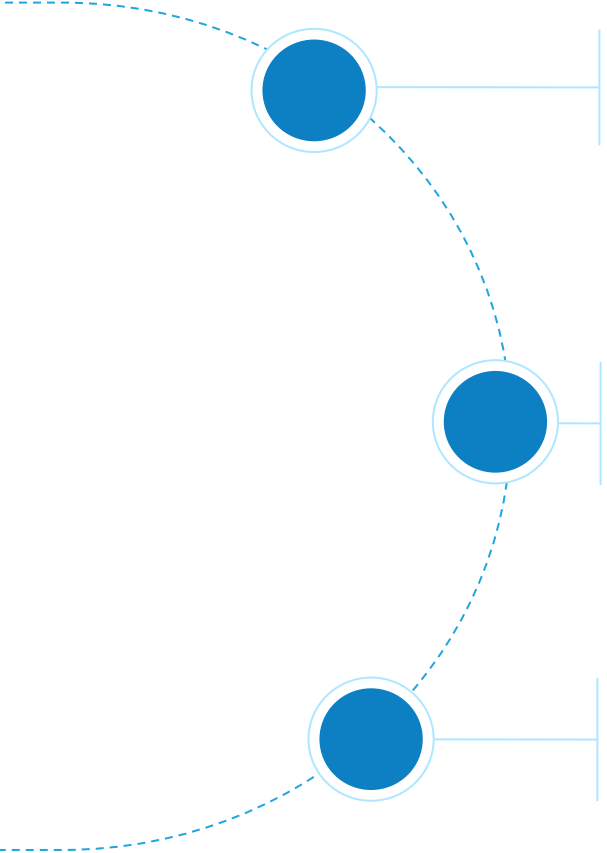
Системный администратор

- Настройка оборудования и ПО
- Контроль работоспособности
- Без доступа к прикладным данным

Бизнес-администратор

- Работа с пользовательскими данными
- Управление правами операторов
- Контроль выполнения прикладных задач
- Без доступа к системным настройкам

ПРАВИЛО «ЧЕТЫРЕХ ГЛАЗ»

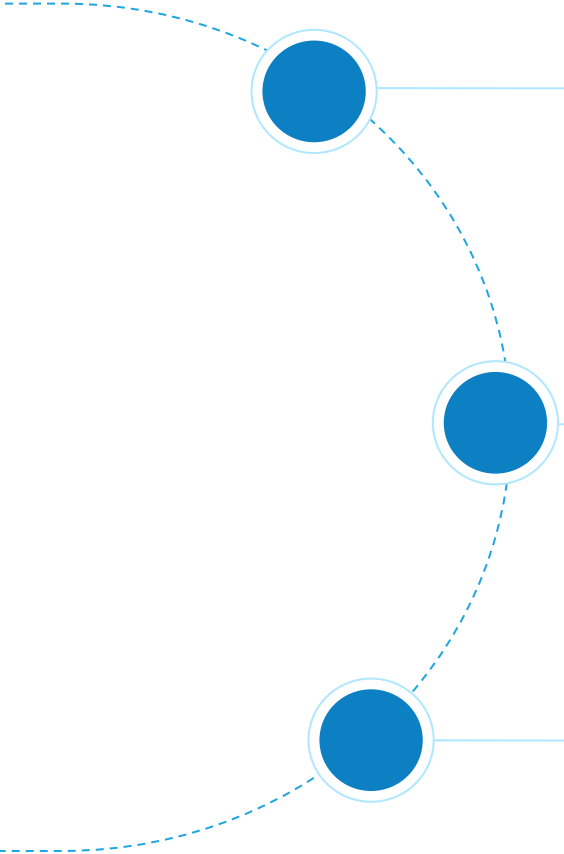


Существенное изменение настроек

Создание нового администратора

Изменение прав администратора

УПРАВЛЕНИЕ ПРАВАМИ ОПЕРАТОРОВ

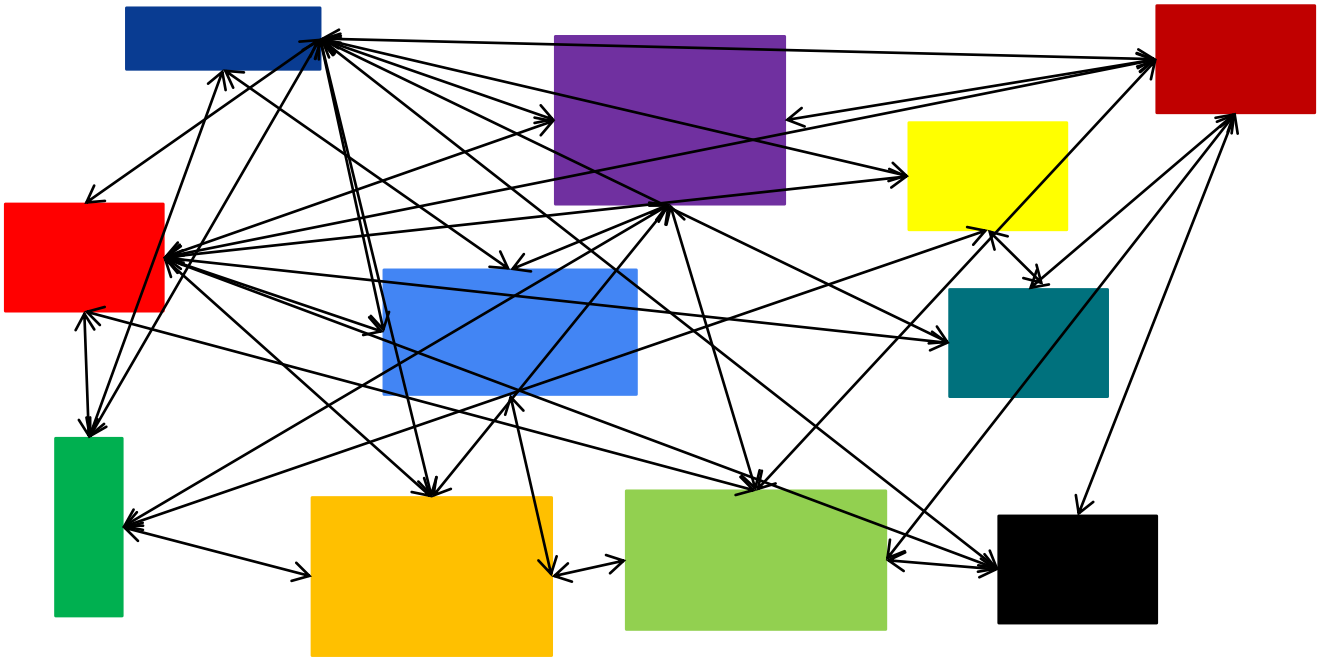


Ролевая модель разграничения доступа к системе

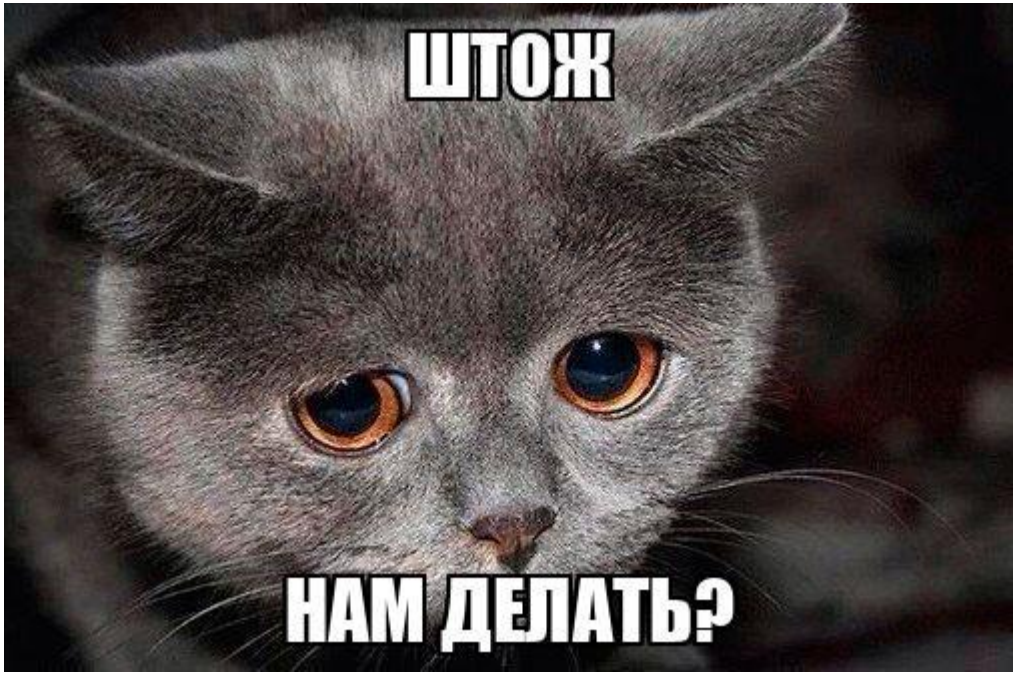
Ограничение возможностей до строго необходимых

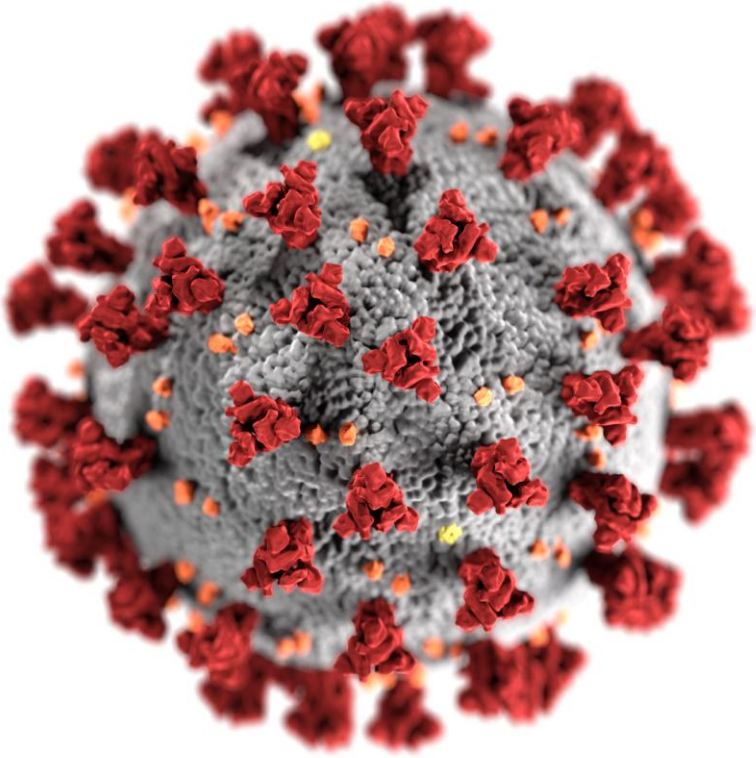
Защита данных от просмотра и копирования

ВНЕШНИЕ СИСТЕМЫ



ЭКСПЛОЙТЫ И ВИРУСЫ





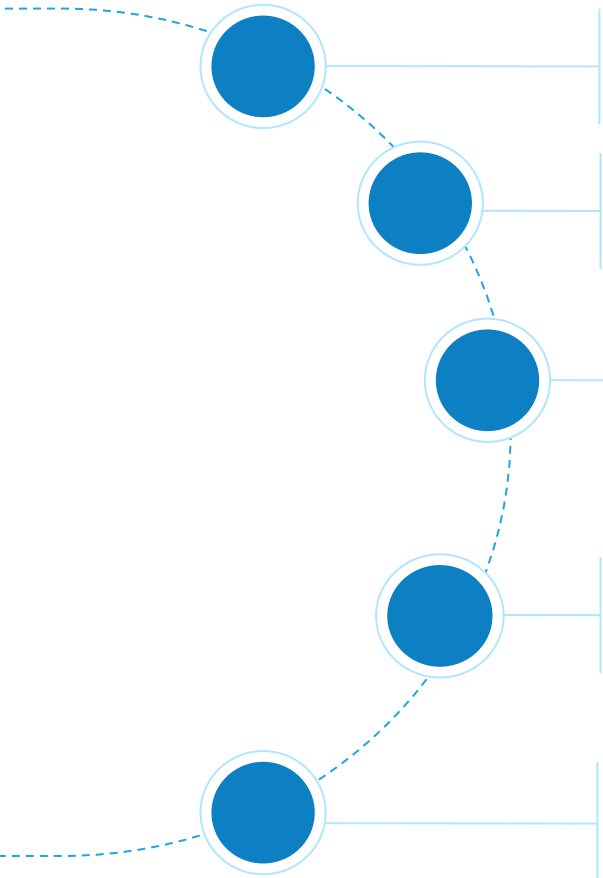
НАЛОЖЕННЫЕ СРЕДСТВА

Антивирусное ПО
Межсетевые экраны…

Ответственность
систем безопасности?
Не мешать!

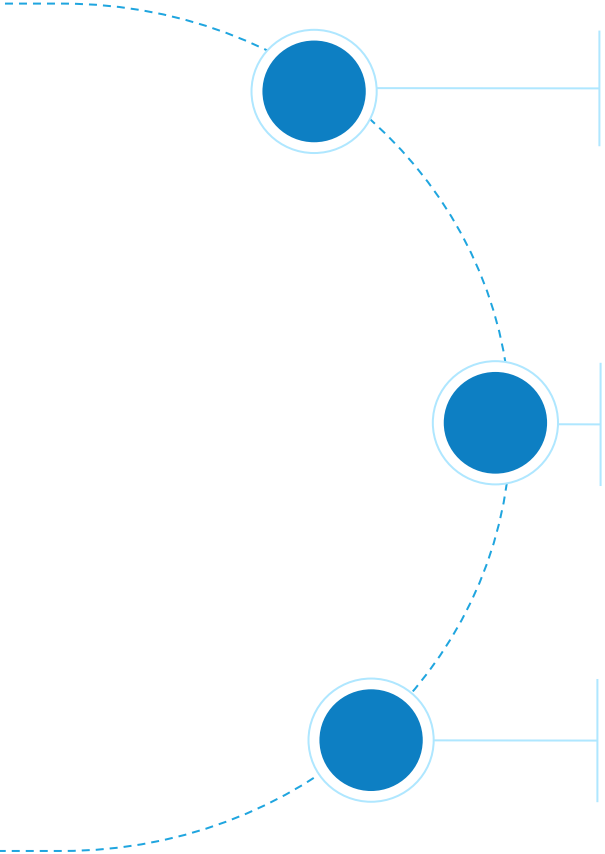
ДАЖЕ LINUX ПОКА «ЛЕКАРСТВО»

ЧТО МЕШАЕТ В БОРЬБЕ С ЭКСПЛОЙТАМИ?



- Устаревшие версии «всего»
- Ограничения/отказ/запрет на обновление ОС
- Ограничения/отказ/запрет на обновление прикладного ПО
- Ограничения в использовании наложенных средств
- Запуск прикладного ПО от имени администратора

НАШ ОПЫТ

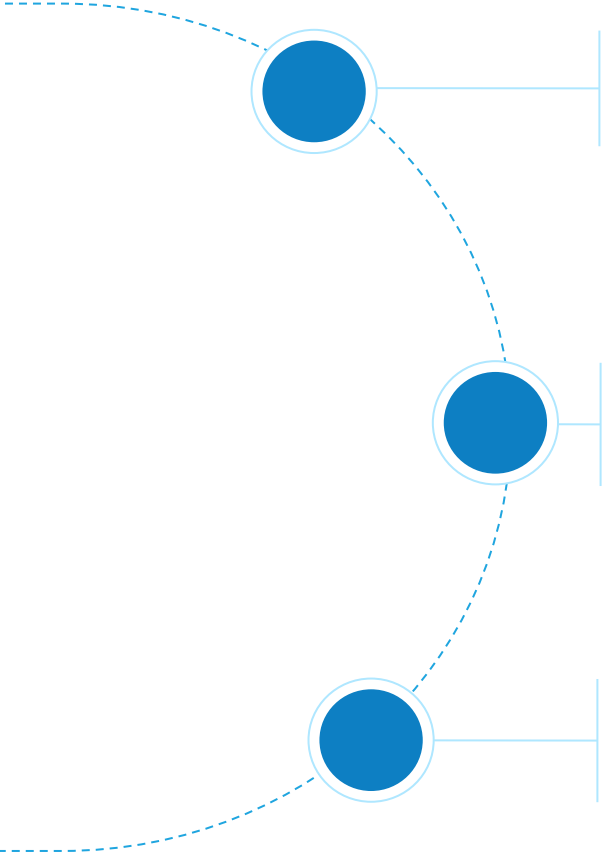


Первое Linux-решение – 2007 год

Первые элементы НЕЙРОСС – в контроллерах с 2014 года

Первый релиз НЕЙРОСС – 2018 год

КАК РАЗВИВАЕМСЯ



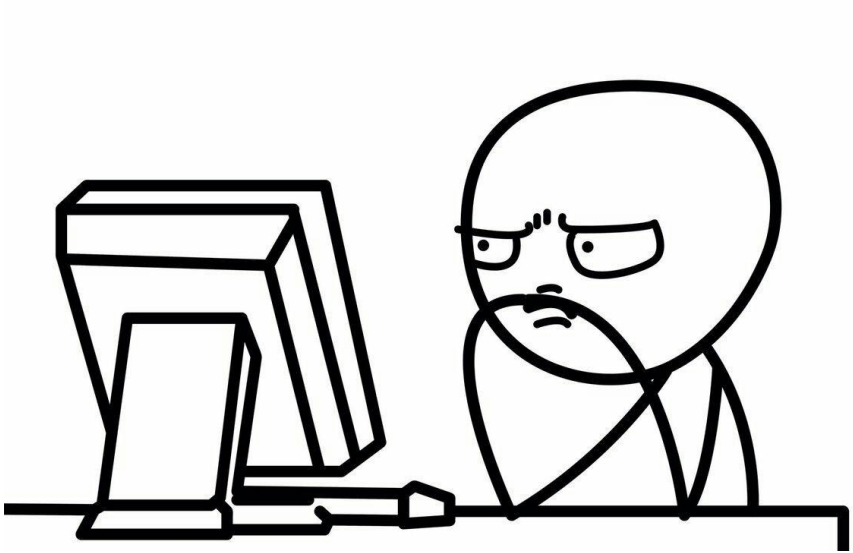
Изоляция прикладного ПО от операционных систем

Единая шина данных с полным протоколированием

Защищенное подключение оборудования, шифрование трафика

ИТОГИ

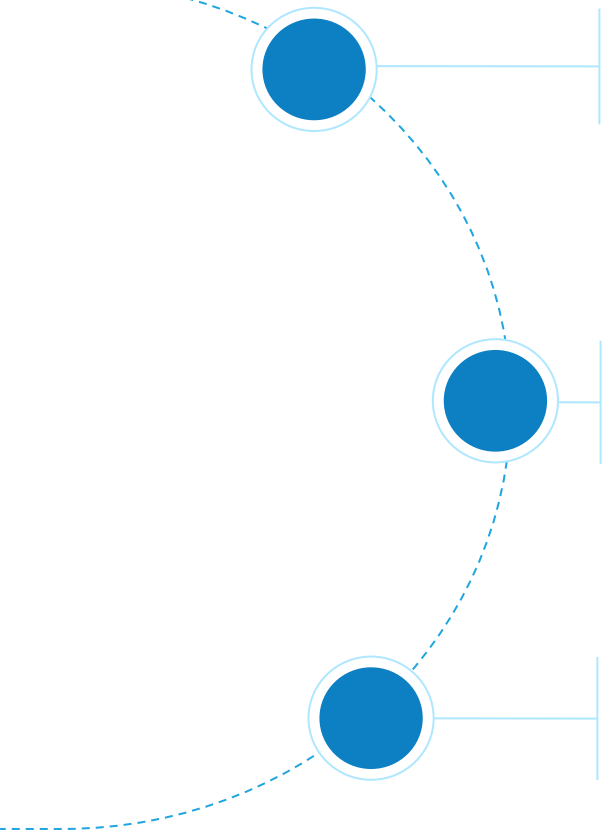
Может, я «на воду дую»?



ГЕОГРАФИЯ АТАК ЗА ОКТЯБРЬ

- 20+ «точек на карте»
- 200+ атак на ресурсы компании

КТО И ЗАЧЕМ?

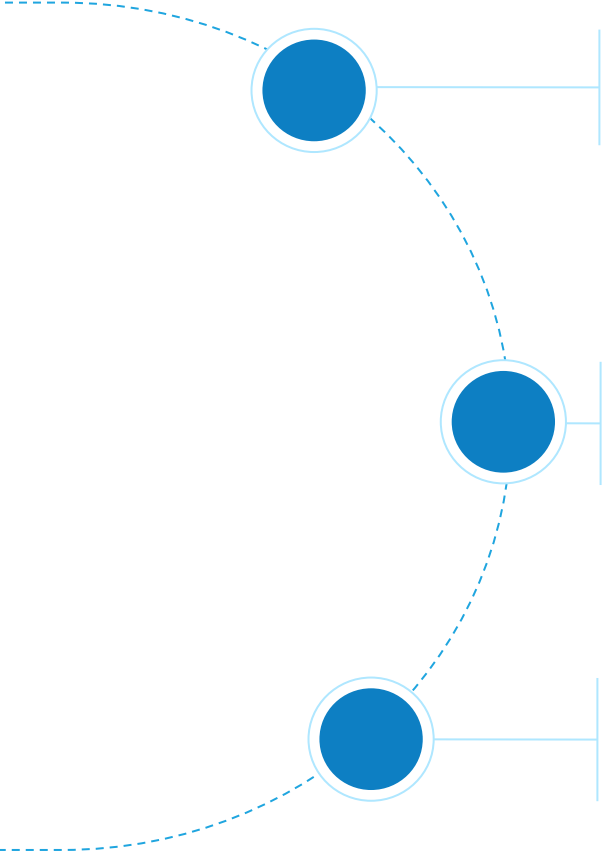


Причинение экономического ущерба

«Идеологические» причины

«Спортивный» интерес

ВЫВОДЫ



Атаки неизбирательны

Вы можете не знать, что вас ломают. Или уже взломали

Киберзащищенность – ответственность и разработчика

ПРОБЛЕМА РЕАЛЬНА

НАД НЕЙ НАДО ДУМАТЬ УЖЕ СЕЙЧАС

И ВЫБИРАТЬ РЕШЕНИЯ, В КОТОРЫХ НАД ПРОБЛЕМОЙ РАБОТАЮТ

Спасибо за внимание!

Денис Иванов

Итриум

+7 (812) 960-06-13

interop@itrium.ru